Into:	00:04	This is Force for Hire, a deep dive into private military contracting and how it's transforming the battlefield. I'm Michelle Harven and I'm Desmond Farris.
New Speaker:	00:12	To be militarily dominant today, it means being technologically advanced. That's why for many Pentagon leaders, the next arms race is in Cyber Cambridge analytics whistleblower Christopher Wiley who exposed digital scandals in the 2016 presidential election and Brexit said the real war is being fought online and as the military modernizes and digitizes often with the private sector's help more vulnerabilities emerge.
Desmon Farris:	00:43	A 2018 Pentagon report found Lockheed Martin's F-35 program, the most expensive weapons system in history , could be susceptible to hackers, but what may be more pressing is systems already in place. An inspector general report found 266 open cybersecurity weaknesses at the Department of Defense, some over a decade old and last year the Defense Department's travel records were breached. Additionally, contractors who work with the government can be a vulnerability. Last year, Chinese hackers stole massive amounts of highly sensitive data from a Navy contractor and when data is internally leaked, we've seen that often done by military contractors. Like the situation with Edward Snowden,
Michelle Harven:	01:29	we sat down with Richard Clark to address cyber security threats and how military contractors have both helped and hurt national security. Along the way. Richard served for 30 years in U.S. government, national security agencies, including the Pentagon, the State Department, and the White House National Security Council. He coauthored the books" Cybersecurity, the next threat to national security and what to do about it" as well as the "fifth domain defending our country, our companies and ourselves in the age of cyber threats."
New Speaker:	02:03	Can we talk for a s just about very general, the cyber threats to our own national security right now. Where do you put the threat level right now?
Richard Clark:	02:12	Well, let's quote the director of National Intelligence. Dan Coats in his, uh, annual threat briefing to Congress where he and the heads of the other intelligence agencies go into an open session, unclassified session in the Congress every year. And they rank order the threats this year. As with last year, they said the number one threat was a cyber attack, cyber attacks from nation states. And they specifically listed, uh, Russia, China, Iran, and North Korea.

Michelle Harven:	02:43	And not only that, you say the next major war will be provoked by a cyber attack is, do you still think that's true?
Richard Clark:	02:52	Yeah, I think it's highly likely that leaders will think they can attack each other in cyberspace. It will stay there. For example, President Trump recently decided to deescalate with Iran. Uh, tensions were building up because they shut down one of our drones. He had the option of attacking or with aircraft dropping bombs and missiles, and instead of the very last minute peak, cancel that and ordered instead of cyber attack. I think that reflects a general attitude on the part of leaders that somehow cyber attacks are not as offensive, that they're cleaner, less lethal, et cetera. But as we know from a past experience, cyber attacks can be as destructive as a missile attack or a bomb attack, uh, and they can be lethal. The Hamas Palestinian group, uh, had been attacking Israel in cyberspace recently. Uh, the Israelis had enough, uh, and say they launched a couple of f sixteens, uh, and bombed the Hamas cyber facility.
Richard Clark:	04:00	I think that's the kind of thing we're going to see in the future where people think they can be safe attacking each other in cyberspace. And then somebody says, oh, enough, uh, we're going to respond with kinetic action. In fact, the Defense Department's official policy, public policy is that if we are hit, we, the United States are hit by a cyber attack that does significant damage and they don't define significant intentionally. They want it left vague. We reserve the right as a nation to respond with a kinetic response, including conventional bombs and missiles. Uh, so I think any war in the future is going to involve a cyber dimension, but there's a high probability that that cyber dimension will go first and people will think they can limit it to that and they'll be wrong.
Michelle Harven:	04:51	And is there also something to say maybe about how easily someone can get a hand on a computer or even a phone. Now they don't have to get weapon, military grade weapons in order to carry out an attack? Is this part of it?
Richard Clark:	05:04	As we, as we discussed in the book, uh, for simple attacks, you can buy them and we actually have a price list. Uh, in the book. Uh, you can go online to various places that some people call the dark web, but you can go online and you can download a what is called a remote access tool or rat, um, for about a thousand dollars. If you want a very sophisticated attack that no one has ever used before, no one has ever seen before, uh, that's called a zero day, uh, because when it's used, it'll be days zero for that attack. If you want as a sophisticated zero day, you

can probably even get that online. And we've seen prices as high as a million dollars for that software. But you don't have to be a sophisticated coder. Uh, you don't have to know a lot computer science, uh, to download these things and press send.

Michelle Harven: 06:01 So the barrier to entry is a bit low.

Richard Clark: 06:04 The barrier to entry is low. If you're attacking a company, uh, or a military organization and government agency that hasn't done a good job. But what we point out in the book, the fifth domain is the barrier to entry. Now, for somebody who wants to attack a sophisticated company is very, very high. The Big Wall Street banks, it may surprise people. There are banks like Bank of America on JP Morgan that are spending a billion with a B billion dollars a year on cybersecurity, uh, and they have on their own staff, 1500, 2000 people doing just cybersecurity for one bank. Uh, good luck getting into that. What we found out, uh, is that in fact the change over the course of the last five years by the introduction of artificial intelligence and machine learning on the defense and, uh, point detection and response software, uh, and micro segmentation of networks, a whole series of new technologies that are really come online in the last five years, it makes it possible if you really spend a lot of money, uh, and you have good people doing it and they're constantly monitoring it and you're constantly updating, we think you can create a secure network, uh, where if somebody gets in, you're going to see it right away and you're going to contain it right away.

Richard Clark: 07:33 And we call that the resilient network that bounces right back. So the barrier to entry has gotten very high, if not insurmountable in some sophisticated companies, not so much in the government, not so much in the military.

New Speaker: 07:47 Do we know how much of the U.S. cybersecurity is handled by government worker versus private companies and contractors?

Richard Clark: 07:55 Well, I think most of it's handled by private companies and contractors. Most government departments and agencies, uh, don't do their own cybersecurity. Uh, they contract it out now that it's not true of cyber command that the cyber command has, has contractors working for it, but they're obviously military people with hands on, uh, keyboards as well. But the, the big change over maybe the last 20 years has been, if you go back 20 years ago, there were a lot of government only products that the government had developed in its labs or the government had contractors developed for it, but only for it, uh, so-called Gods, uh, products and government off the shelf

systems in cybersecurity. That's not true anymore. There are very, very few defensive, uh, software programs, applications that only the government has. Fact, I'm not sure there are any, if you go on to any government that work in the Defense Department, the State Department or the Agriculture Department, uh, you're going to find the same products, uh, that are running, uh, on j p Morgan or Bank of America or Citibank.

Richard Clark: 09:13 What's interesting about that is that if we go back again to JP Morgan, three years ago, they were running 75 different software programs to defend the network, 75 different applications for, to do specific things about defense. When I started in this business in 1997, you can only buy three things. You could buy a firewall and you could buy an antivirus system, uh, and you could buy something called an intrusion prevention system. I remember in 1997, the deputy secretary of defense ordered army, navy, air force, marines all to install intrusion prevention systems in a rush right away, big emergency and get them installed. And then about six months later we met, uh, with the various military departments and ask them, uh, how, how's it going with these new intrusion prevention systems? And we had an Army general who had said they're a real pain in the rear, uh, before we installed these systems.

Richard Clark: 10:20 Um, no one ever attacked us. Uh, and now that we have these intrusion detection systems on board, uh, we're getting a a hundred, uh, attacks a day. Well, obviously the for a hundred attacks a day before they installed the systems, still he just didn't know it. But my point is you can only buy those three things, firewalls, a v Antivirus and intrusion detection. Now you can buy and you kind of have to buy if you're really going to secure the network, dozens of different products, each doing a specific thing, each worried about the specific way that somebody could attack the network. And if you do that you can achieve reasonable degrees of success. Does that mean it kind of cybersecurity already started in the private sector? Um, I would say started in the private sector. No, it started in this, say like a as Fort Meade, but it's certainly now almost entirely in the private sector and the products, uh, whether the products are on a destroyer or on the bank, the products are all the same and they're on the, probably on a British destroyer and the Russian destroyer there.

Richard Clark: 11:29 Uh, the export of the defensive software is not controlled by the State Department as a weapon. Uh, it's just sold commercially around the world. There are no controls on who gets it other

than the normal sanctions that you can't do business with certain countries, uh, at all. But there are no controls on the products. The products are all, um, developed largely with venture u s venture capital money rather than with government research money. And originally the defense, uh, advanced research projects, agency DARPA did a lot of the funding for research and Development in cyberspace. Now it's done by us venture capital firms that fund startups.

Michelle Harven: 12:14 Is that all worrisome? That it's a lot of this is being evolved and taking control of by the private market?

Richard Clark: 12:21 Well, the government couldn't do it, so I don't, I don't see any, a real alternative to it. Uh, there's no government agency that could foster the, uh, the kind of a startup culture and innovation, uh, and research, even if the government did it, it would just outsource it to a, to a university to do. And frankly, having the venture capital world funded makes it move faster because the, all of those people in these little startups who are creating new cybersecurity products are highly incentivized personally. They're going to make a lot of money if their product works. And so I know these people, they work themselves to death, creating these products and getting them to market and then they make, they do make a lot of money if that product works, but they've sacrificed three, five years of their lives, never seeing their family working on weekends. It's a, there's something to the capitalist system of getting stuff done quickly if you incentivize people.

Michelle Harven: 13:24 When we come back, the challenges in securing government data when employing contractors and much more.

New Speaker: 13:32 Stay informed on all the news that matters most to the military community with a subscription to Stars and Stripes digital access. As a subscriber, you'll enjoy unlimited access to the stripes.com website and our Stars and Stripes mobile apps updated 24 seven by reporters stationed at military bases around the globe. Subscribe today and enter the Promo Code podcast when signing up for a yearly subscription and receive 50% off your first year. Get exclusive access to special features, interactive articles, award-winning photography and more. Visit stripes.com/digital and enter the promo code "podcast" to subscribe today.

Michelle Harven: 14:28 So we've talked about how contractors or the private sector can help the Defense Department with cybersecurity. There's also contractors working in the military who could be seen as sort of

vulnerable targets for hackers. Yes. And there was a last year Chinese hackers stole data on a new anti-ship missile from a navy contractor and the data was stolen even though it was on this contractor is unclassified network and that that data apparently was highly sensitive. Did you have any sort of takeaway from this incident?

Richard Clark: 15:02 Yeah, I think there's a real lack of adequate security on the part of both the government agencies that are using contractors and the contractors themselves. We've seen numerous incidents, contractors downloading sensitive information off government networks onto their personal laptops and then taking them home. Now that may be innocent in some cases they want to work on the weekends or they want to work from home, but it's enormously risky when you're on the government network and at least in theory, there's a lot of protection around that government network. A lot of security around that government network and you take it home, there's no security on your personal laptop burning on the Wifi at Starbucks or you know, running into, in your, in your playroom at home. And we've seen, this is not theoretical. We've seen this happen. When Edward Snowden, who was a contractor for Booz Allen, downloaded just reams of sensitive information from NSA.

Richard Clark: 16:05 Uh, no alarms went off. He stole credentials or borrowed credentials from supervisors. No alarms went off. Uh, there were no two factor off authentications, um, systems in a forest. So President Obama at the time asked me and for other people to investigate why it was that it was that easy to steal information from what supposed to be our most secure government agency. And we said in an unclassified report to the president, which was published, uh, that NSA had been extraordinarily lax in its own security and particularly when it came to contractors. Uh, and we had a whole series of proposals for background checking, you know, on a continuous basis, personnel with eligibility to see sensitive information and continuous monitoring of the network to see if anybody is doing something funny like downloading massive amounts of sensitive information. I think those recommendations have been generally implemented, but even after, oh, they shouldn't have been implemented. There have been incidents,

Michelle Harven: 17:15 well, in fairness, the government is trying to secure its data when employing contractors, the National Institute of Standards and Technology announced plans for new contractor's cybersecurity standards not implemented yet. Yep. Although a year after contractors were required to secure Defense

Department data, there were reports of confusion and misunderstanding about the mandate. What are the challenges here? Why do you think there are so many challenges with this?

Richard Clark: 17:41 I think the challenge is one of the management priority. Every manager, every commander has any mission. Uh, and most them are not. Most of the missions are not cybersecurity. Uh, they've commissioned to do x or y, uh, and they have, you know, collateral duty to make sure that there's good cybersecurity. Like they have a collateral duty to make sure this, you know, a healthy work environment and all sorts of other things. Uh, they don't take it seriously. They don't realize that they are risking lives. I believe that because of the information that this fellow Snowden, uh, gave to the Russians, uh, and released on the web so the terrorist groups could read it. I think it's highly likely that lives were lost. Cybersecurity, uh, sounds like a minor administrative thing to some people. It's a pain in the rear end. You know, you're gonna Change your passwords and you gotta do all that.

Richard Clark: 18:34 It is as important as any mission we have to defend our country. And one little mistake that someone makes along the way can be utilized by the enemy. And we do have enemies, uh, and we are in the cyber war, low grade, but nonetheless, we are in the cyber war. Any little mistake that anyone makes can be at the opening that the enemy needs to get in and do extraordinary damage. The information they get can reveal undercover agents can reveal the ways that we find and prevent terrorist attacks. It can reveal vulnerabilities of weapon systems. There are all sorts of things that you can lose. Uh, when you lose just a few digits.

Michelle Harven: 19:15 There was a report this year by the New York Times on what they call Internet mercenaries conducting cyber warfare for foreign governments and they cited places like Saudi Arabia or Qatar. How do you see the cyber techs being used as sort of digital combat.

Richard Clark: 19:33 Well, I think as it is true that there are teams, cyber teams that you can hire if you're a country that hasn't been able to indigenously produce a cyber command of your own, there are people for hire. Some of those people are people who work for the Chinese army during the day or the Russian Gru and Russian military intelligence during the day and or during the night or weekends, they moonlight as part of a cyber gang or team. Let's for hire, and we've seen this, you've seen this happen with North Korea. They've seen it happen with China, with Russia and other countries that criminal activities occur by very

sophisticated attacks by the same people who worked during the day for the government. So, yeah, it is possible. There are such things as a, you can call them cyber mercenaries. Uh, some of them work for the government, uh, during the day. Some of them don't. Some of them are just really good hackers. We've always been concerned in the United States that al Qaeda or Isis, uh, would one of these teams and do damage in cyberspace. So far from everything we know, every time the terrorist groups have tried to hire hackers, uh, the dares groups have said no. Uh, so maybe there's some honor among thieves after all.

Michelle Harven: 21:03 Well, it does seem that you need to layer them away with a high salary in order for them to conduct that sort of work. There were reports of former CIA and NSA employees with experience in offensive cyber operations being tempted by foreign cyber firms, particularly an MRA from dark matter. There were talks that these agencies should ensure that their employees can't use their experience against the United States.

Richard Clark: 21:30 Well, uh, there, there are laws and anyone involved in contracts with o with foreign entities need to be breached on these laws so that they realize that you can't just go to work for a foreign entity with knowledge that you had, uh, in the u s government or an eos government contract and everybody is supposed to be briefed about what those laws are. It turns out that as individual American, you cannot hack into another network that's a, that's a felony. It's a violation that computer fraud and abuse act. That's true. Even if you do it on the moon, it's true. Even if you do it in London, so you can't say, oh, I'm going to go to London and worked for a British company and hack into other networks. If you're an American, it's illegal or ever you go, it's illegal to hack into another network unless you have permission of the u s government.

Michelle Harven: 22:32 How much of the cybersecurity in tech talent is learned away to higher paying firms in Silicon Valley and elsewhere? It's

Richard Clark: 22:40 very, very hard. The, for the military and the federal agencies or state agencies for that matter to get people to go to work for them in cybersecurity because it just can't pay on, uh, military salaries or civil servant salaries, which is why very often in the military or civilian agencies have to hire contractors because the contractors can pay more and the contractors can pay a competitive salary to what somebody would get if they were working at the bank. We've tried over the years to deal with that a workforce problem by creating something called cyber

core. The cyber core is a great program where there, I think now 80 colleges and universities and community colleges around the country where you can go and for two years the u s government will pay tuition and all your expenses and give you a stipend to live on if you study cybersecurity and if when you come out of college, you worked for the u s government or a state local or tribal government for one year, for every year he took the, the scholarship.

Richard Clark: 23:53 So the most you can get is the two year scholarships. So you'd only have an obligation to work for two years for the government. And this program has been running since the Clinton administration. And what we've seen happen is a lot of people, once they get in the government love the mission, uh, and even though the pay is less and they stay, and so we've had really good retention rates in cyber core, but if anybody is listening and thinking about going to school, studying cybersecurity, check out the scholarship for service cyber core and see if you can get into one of the certified programs at one of the, uh, universities and colleges that, and now community colleges that have the program.

Michelle Harven: 24:36 And I do wanna mention that cybersecurity is a huge market. There are five US defense contractors are among the world's top 25 cyber security companies and cyber crime costs the world $6 trillion annually. And that's by, by 2021 which apparently is more profitable than the global trade of all major illegal drugs combined.

Richard Clark: 24:58 Yeah, that's amazing. So with drugs, of course people get shot and on, there are dramatic pictures, uh, and therefore we all know about that. Uh, the drug gangs fighting each other and Latin America and whatnot. But you're right, all the estimates are that cyber crime, which is quiet and silent and invisible steels more money than the drugs do.

Michelle Harven: 25:22 How do you see the private sector working with the military, that government from here on out with cyber security?

Richard Clark: 25:28 Well, the private sector frankly is out to make money and they will do as little as they need to do to comply with the contract. Uh, and so the government's got to be really, uh, good about specifying the levels of security it wants those contractors to achieve. And then the government needs to get third party auditors to make sure that they're doing it and continuous monitoring of those contractors. I think the contractors record use such that we can't trust them to do cybersecurity alone

		without somebody watching them and that someone should be the government, but it can also be the government supported by private sector. Third party auditors.
Desmon Farris:	26:17	Thanks to Richard Clark for talking with us to learn more, grab his book, the fifth domain and catch Richard on his own podcast. Future state about the intersection of technology, politics and national security. We're nearing the end of our series with just two episodes left, so you won't want to miss our last story from a contractor.
Michelle Harven:	26:37	In the next episode we hear from Norelle Joyce or as she's also known, mercenary mom is an Australian contractor who began in the service but wasn't given the same opportunities as her male counterparts, so she decided to switch careers.
Norelle Joyce:	26:54	It was pretty hard to take watching my troops deployed to Iraq and even being part of the training team, training them for ops overseas and then I couldn't go myself. So it was after the first lot of treats return back, and they told me about the burgeoning private security contractor saying that was exploding over there in Iraq that I began to seriously look at transferring to a private army.
Desmon Farris:	27:26	Don't forget to subscribe and while you're there leave us a review. You can also let us know your thoughts podcast@stripes.com also, follow us on Twitter for updates @starsandstripes.
Michelle Harven:	27:38	Force for Hire's supervising editors are Bob Reid and Terry Leonard. Digital Team lead and editor is Michael Darnell.
Outro:	27:45	Thanks for listening. This is Force for Hire.